

UNITED STATES DISTRICT COURT

for the
WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of

(Briefly describe the property to be search)

Or identify the person by name and address)

PROPERTY KNOWN AS:

Case No: M-22- 853-SM

1. a red SanDisk 4GB SDHC card;
2. a Samsung cell phone in a red and black case;
3. a dark Galaxy S10e;
4. a dark iPhone in a Lifeproof case;
5. a green and black Seagate Xbox external hard drive,
S/N: NZ0E87HL
6. a dark Alcatel flip phone;
7. a SanDisk USB thumb drive with a Samsung
USB-C adapter;
8. a gray Lenovo laptop Model IdeaPad 5,
S/N: PF2E5BTN; and
9. a dark Galaxy J7 in an OtterBox case

IN POSSESSION OF:

Pottawatomie County Sheriff's Office Criminal
Investigative Division
One John C Bruton Boulevard, Shawnee, Oklahoma

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property (*identify the person or describe property to be searched and give its location*):

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is (*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. §§ 2252 and 2252A

Offense Description

Possession and Distribution of Child Pornography

The application is based on these facts:

See attached Affidavit of Special Agent Brian Cunningham, Homeland Security Investigations, which is incorporated by reference herein.

☒ Continued on the attached sheet(s).

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).



Applicant's signature

BRIAN CUNNINGHAM

Special Agent, Homeland Security Investigations

Sworn to before me and signed in my presence.

Date: November 22, 2022



Judge's signature

City and State: Oklahoma City, Oklahoma

SUZANNE MITCHELL, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Brian Cunningham being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I have been a Special Agent (SA) with Homeland Security Investigations (HSI) since December 2010. I have specific training and experience in numerous methods of investigation, including, but not limited to, electronic and visual surveillance, general questioning of witnesses, the use of search warrants, the use of confidential sources/informants, the use of pen registers, and the use of undercover agents. Based on my training and experience relating to the investigation of child pornography and based upon interviews I have conducted with other officers, defendants, informants, and other witnesses and participants in child exploitation, I am familiar with the ways that child pornography is manufactured and distributed. My familiarity includes the various means and methods by which producers of child pornography manufacture and distribute pornography, including their use of cellular telephones and computers. Additionally, I have observed, reviewed, and identified thousands of child pornography images and videos (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a Deputized Homeland Security Investigations Task Force Officer who is engaged in enforcing criminal laws, including 18 U.S.C. § 2252 and 2252A, and I am deputized to request and execute search warrants.

2. The statements contained in this affidavit are based in part on information provided by law enforcement officials and others known to me, and on my own experience and background as a law enforcement officer. Since the affidavit is being submitted for the limited purpose of establishing probable cause, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that violations of Title 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography) and 2252(a)(2) (distribution of child pornography) have been committed and that the instrumentalities, fruits, and evidence of those crimes will be found in a particular place to be searched.

3. This affidavit is made in support of a search warrant for the following items (“DEVICES”), which are currently in the legal custody of the Pottawatomie County Sheriff’s Office Criminal Investigative Division and located in their secure evidence storage room at One John C Bruton Boulevard, Shawnee, Oklahoma:

- a. a red SanDisk 4GB SDHC Card;
- b. a Samsung cell phone in a red and black case;
- c. a dark Galaxy S10e;
- d. a dark iPhone in a Lifeproof case;
- e. a green and black Seagate Xbox external hard drive, S/N: NZ0E87HL;
- f. a dark Alcatel flip phone;
- g. a SanDisk USB thumb drive with a Samsung USB-C adapter;

- h. a grey Lenovo laptop Model IdeaPad 5, S/N: PF2E5BTN; and
- i. a dark Galaxy J7 in an OtterBox case.

I am submitting this affidavit in support of a search warrant authorizing a search of the DEVICES (also described in Attachment A to this affidavit) and the extraction from the DEVICES of electronically stored content and information described in Attachment B hereto, which content and information constitute instrumentalities, fruits, and evidence of the foregoing violation.

DEFINITIONS

4. The following definitions apply to this Affidavit and Attachment B:

a. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other

means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and

connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. “Encryption” is the process of converting data into a code in order to prevent unauthorized access to the data.

h. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the

Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

j. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

k. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

l. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

m. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

n. A “storage medium” or “storage device” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, “thumb,” “jump,” or “flash” drives, CD-ROMs, and other magnetic or optical media.

o. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

p. A “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

PROBABLE CAUSE

5. From August 26, 2022, to September 23, 2022, Pottawatomie County Sheriff’s Office (PCSO) Lieutenant Steven Sample conducted online downloads on the

BitTorrent network looking for individuals in Oklahoma who were engaged in the receipt, possession, and distribution of child pornography. Lieutenant Sample identified an electronic device in Oklahoma using the IP address 8.40.161.126. The user of the IP address made available for download numerous files containing child pornography, which specifically include images and videos of pre-pubescent children exposing their genitals and adult males penetrating pre-pubescent children. The IP address 8.40.161.126 was the sole provider of data for each download, and as such, each file was downloaded directly from this IP address. A total of 47 different connections were made to the IP address and each download, conducted by Lieutenant Sample, netted multiple images and videos of child pornography.

6. BitTorrent is a Peer to Peer (P2P) network. P2P file sharing allows people using P2P software to download and share files with other P2P users using the same or compatible P2P software. P2P software is readily available on the Internet and often free to download. Internet connected devices such as computers, tablets, and smartphones running P2P software form a P2P network that allow users on the network to share digital files. BitTorrent is one of many P2P networks. For a user to become part of the BitTorrent network, the user must first obtain BitTorrent software and install it on a device. When the BitTorrent software is running and the device is connected to the Internet, the user will be able to download files from other users on the network and share files from their device with other BitTorrent users.

7. Users of the BitTorrent network wishing to share new content will use a BitTorrent program to create a “torrent” file for the file or group of files they wish to share. A torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Torrent files are typically found as the result of keyword searches on internet sites that host or link to them. Torrent files may be referenced by their “infohash”, which uniquely identifies the torrent based on the file(s) associated with the torrent file.

8. On Friday, September 23, 2022, a query was made on the IP address 8.40.161.126 through the American Registry for Internet Numbers (ARIN). ARIN reported the IP address 8.40.161.126 was registered to Allegiance Communications, LLC, a subsidiary to Vyve Broadband.

9. On September 23, 2022, after review from Judge Emily Mueller, a State of Oklahoma Title 18 order requesting the identity of the internet subscriber for IP 8.40.161.126 from August 26, 2022, to September 23, 2022, was authorized and submitted to Vyve Broadband.

10. On September 28, 2022, a response from Vyve Broadband stated the subscriber for IP address 8.40.161.126 during that timeframe was Marissa Hair. The response listed Marissa Hair’s address as 112 Jack Rabbit Drive, Shawnee, Oklahoma. Subsequent database checks and research conducted by Lieutenant Sample identified two

possible residents of 112 Jack Rabbit Drive as Marissa Hair and Cody HARRIS. Further record checks showed Marissa Hair and Cody HARRIS were married on August 3, 2020.

11. On September 27, 2022, Lieutenant Sample applied for and received an Oklahoma State search warrant for 112 Jack Rabbit Drive based on the above information. On October 3, 2022, Lieutenant Sample executed the search warrant with the help of the Pottawatomie County Fugitive Task Force (FTF) and Homeland Security Investigations (HSI).

12. Marissa Hair and Cody HARRIS were located inside the residence during the execution of the search warrant. After the house was secured Lieutenant Sample and I spoke with both Marissa Hair and Cody HARRIS. Lieutenant Sample explained that he had a search warrant for the house because someone at the home had been downloading and distributing child pornography. While making that statement investigators were watching for any subconscious or nonverbal clues of who may been involved. Marissa Hair broke down into a panic attack and had a look of complete shock on her face. HARRIS looked as if he had the wind knocked out of him, looked down at the ground, and turned his head away from everyone without saying anything. Marissa Hair asked HARRIS if he did it. HARRIS repeatedly reached over to touch Marissa Hair and comfort her. Marissa Hair pulled away and shouted, "Stop Touching Me!"

13. Lieutenant Sample then asked HARRIS to come back to his vehicle to talk which he agreed to. Lieutenant Sample read HARRIS his Miranda which was witnessed

by me. HARRIS agreed to speak with the investigators. Lieutenant Sample asked HARRIS if he knew what a torrent was, and he stated he did. Lieutenant Sample then asked HARRIS to explain what a torrent was in his own words. HARRIS said you just go to Google and type in torrent and what your looking for. Lieutenant Sample asked Cody if anyone other than Marissa Hair and him live at the house. HARRIS stated that no one else lived at the house. Lieutenant Sample asked if he shares the WIFI password with any neighbors or anyone that comes to the house a lot. HARRIS said they did not share the WIFI password. Lieutenant Sample asked if he downloaded any of the child pornography torrents mentioned earlier. HARRIS stated no. I then asked Cody if he would be willing to take a polygraph to clear his name of any involvement and or any hands-on offenses and he agreed to the polygraph examination.

14. Lieutenant Sample and I drove HARRIS to the Pottawatomie County Sheriff's Office Criminal Investigative Division office and met with Oklahoma Highway Patrol Trooper McKey who conducted the polygraph examination. Trooper McKey first tested HARRIS on any hands-on offences with minors. HARRIS's results showed Trooper McKey that he was being honest and had not been a hands-on offender with children. HARRIS then agreed to take a second polygraph examination regarding the downloading of child pornography. Trooper McKey conducted the exam and concluded that HARRIS had failed. Trooper McKey then informed HARRIS he had failed the polygraph regarding downloading child pornography. Trooper McKey told HARRIS that for most of human

history younger girls were more desirable and sought after because they were more fertile. It was just in the last 50 years or so a man being interested in a girl under the age of 18 had become taboo. HARRIS nodded his head yes a couple times, as if he was agreeing, while Trooper McKey was making this statement. Trooper McKey asked HARRIS if there was anything else he wanted to talk about. HARRIS said he could not say anything else without an attorney and all questioning was ended.

15. After the polygraph examination, HARRIS was arrested. HARRIS has been charged with child pornography related offenses in the District Court in and for Pottawatomie County, Oklahoma, Case No. CF-2022-00393.

16. Lieutenant Sample and I contacted the HSI agents who were still at the residence by phone to find out what Marissa Hair had said in her interview. Marissa Hair told agents she had first met HARRIS when she was 13. HARRIS was 20 at that time and was dating and messing around with several of Marissa Hair's friends who were also 13. Marissa stated she had been having issues with her internet lately and, the Monday before, she had to upgrade the internet to a higher speed as she could not connect to her VPN on her work computer. Marissa Hair contacted her work's IT department who told her she did not have enough bandwidth. Marissa Hair also stated that HARRIS used two cellphones. He used one cell phone to download movies on. She went on to say that HARRIS primarily used Duck Duck Go for a search browser. [Duck Duck Go is a privacy

search browser that is designed, so internet sites are unable to track your location and the content you are searching.]

17. Lieutenant Sample and I went back to the residence and spoke to Marissa Hair to ask additional questions. Lieutenant Sample asked Marissa Hair if she knew what a torrent was. Marissa Hair had no idea what a torrent was. Marissa Hair then handed the investigators what she believed to be a SD card she found in the living room. She said she was afraid it was missed during the search and was concerned that it could contain child pornography. Lieutenant Sample saw that it was a SD card adapter which contained no data.

18. The DEVICES were seized from the residence during the search warrant. Based on the statements of Marrisa Hair, HARRIS had access to all of the DEVICES prior to the search and seizure.

19. The DEVICES are currently in storage at the Pottawatomie County Sheriff's Office Criminal Investigative Division evidence room located at One John C Bruton Boulevard, Shawnee, Oklahoma. In my training and experience, I know that the DEVICES have been stored in a manner which its contents are, to the extent material to this investigation, in substantially the same state as they were when the DEVICES were seized from HARRIS.

COMPUTERS, THE INTERNET AND CHILD PORNOGRAPHY

20. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

- a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.
- b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard

drive in the camera. The video files can be easily transferred from the camcorder to a computer.

- c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP's) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (*i.e.*, "instant messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.
- d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Given the storage capabilities, modern computers can retain many years' worth of a

user's data, stored indefinitely. Even deleted data can often be forensically recovered. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person or in their immediate vicinity. Digital files can be quickly and easily transferred back and forth between computers (as broadly defined by 18 U.S.C. § 1030(e)) and other digital file storage devices or stored simultaneously on them. For example, smartphones can often synch with a traditional desktop or laptop computer. This can result in files being transferred from the smartphone to the computer or even stored on both devices simultaneously. Thus, I am requesting to seize and copy all electronic storage media on the DEVICES and search them.

- e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. For example, distributors of child pornography can use membership-based/subscription-based Web sites to conduct business, allowing them to remain relatively anonymous.
- f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can usually be found on the user's computer or external media.
- g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally: the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client

software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data. Thus, if a user has downloaded image files, viewed them, then deleted them, a computer forensic examiner could oftentimes find evidence of such actions and maybe even the deleted images themselves.

SPECIFICS OF SEARCH AND SEIZURE OF DEVICES

21. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying all computers and electronic storage media on the DEVICES that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

22. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with

whom I have had discussions, I know there are certain characteristics common to individuals who distribute, possess, and/or collect child pornography:

a. Child pornography collectors usually start collecting child pornography by obtaining free images and videos of child pornography widely available on the internet on various locations and then escalate their activity by proactively distributing images they have collected, often for the purposes of trading images of child pornography with others, as a method of adding to their own collection of child pornography.

b. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

c. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

d. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years. Collectors prefer not to be without their child pornography for any prolonged time period.

e. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the collector to view the collection, which is valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

f. Child pornography collectors also may correspond with and/or meet others to share information and materials; keep correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Importantly, evidence of such activity, including deleted child

pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.¹

h. In light of the aforementioned, including the facts that demonstrate HARRIS possessed and distributed child pornography, I think (based on my training and experience) that it is highly probable that HARRIS is a child pornography collector.

23. Based on the evidence in this investigation, I believe that HARRIS, likely displays characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography.

¹ See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

CONCLUSION

24. Based upon the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the foregoing criminal violations are located in the DEVICES; therefore, I seek a warrant to search the DEVICES for the items listed in Attachment A.



Brian Cunningham
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 22nd day of November, 2022.

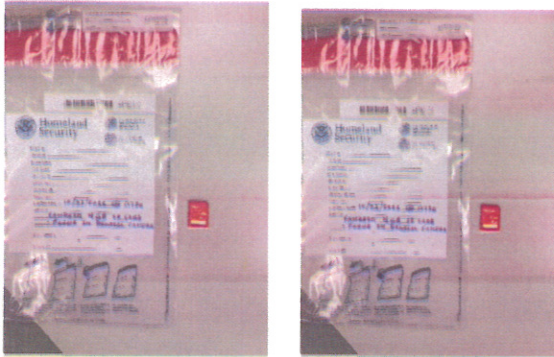


SUZANNE MITCHELL
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

ITEMS TO BE SEARCHED

1. A red SanDisk 4GB SDHC Card;



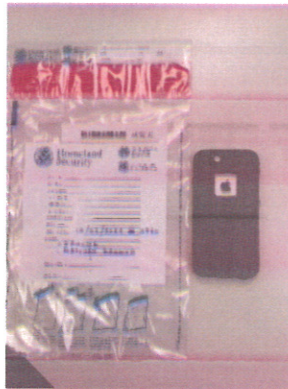
2. a Samsung cell phone in a red and black case;



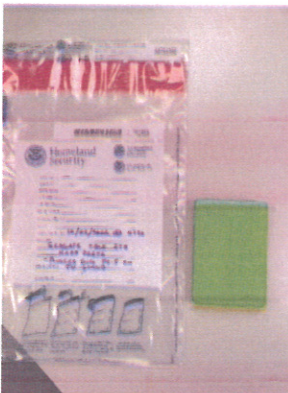
3. a dark Galaxy S10e;



4. a dark iPhone in a Lifeproof case;



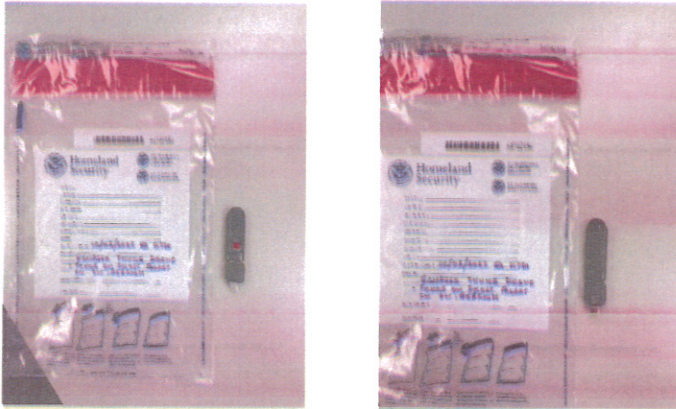
5. a green and black Seagate Xbox external hard drive, S/N: NZ0E87HL;



6. a dark Alcatel flip phone;



7. a SanDisk USB thumb drive with a Samsung USB-C adapter;



8. a gray Lenovo laptop Model IdeaPad 5, S/N: PF2E5BTN; and



9. a dark Galaxy J7 in an OtterBox case.



This warrant authorizes the forensic examination of the DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Any and all digital notes, documents, records, or correspondence pertaining to the possession of child pornography as defined in 18 U.S.C. § 2256(8).
2. Any and all digital images of child pornography as defined in 18 U.S.C. § 2256(8).
3. Any and all digital notes, documents, records, or correspondence identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8).
4. Any and all digital notes, documents, records, or correspondence concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8).
5. Any and all digital notes, documents, records, or correspondence concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.
6. Any and all digital notes, documents, records, or correspondence concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.
7. Any and all digital records, documents, invoices and materials that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection

to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

8. Any and all digital address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8).

9. Any and all records tending to identify the owner or user of the DEVICES described in the affidavit.

10. Any and all diaries, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

11. Any and all records pertaining to how the user of the DEVICES acquired or disseminated any child pornography.

12. Any and all records pertaining to a sexual interest in children.

13. Any federal law enforcement officer may perform or assist with the search for the aforementioned items, including representatives of the United States Attorney's Office.